THE PROLIFERATION OF WIRELESS DEVICES AND ITS EFFECTS ON CORPORATE GOVERNANCE

Ronald Mulder [a] and Rossouw von Solms [b]

[a] Faculty of Engineering, Department of Information Technology, Nelson Mandela Metropolitan University, South Africa
[b] Faculty of Engineering, Department of Information Technology, Nelson Mandela Metropolitan University, South Africa

[a] ronnie@nmmu.ac.za, +27 41 504 3574, Private Bag X6011, Port Elizabeth, 6000
[b] rossouw@nmmu.ac.za, +27 41 504 3604, Private Bag X6011, Port Elizabeth, 6000

ABSTRACT

This paper discusses the need to consider possible risks to ensure business survival and business continuity before the implementation of new technologies, with specific interest to wireless networks and wireless devices. Information Technology is fast becoming essential within business processes and is considered a technical issue yet neglected at board level. In recent years, there has been an elevated awareness in Information Security and Corporate Governance. Organisations, and their board of directors, have become increasingly aware that securing information is vital for the organisation in both financial terms and corporate identity. Wireless Networks, and the use of mobile devices, are bringing the world a new means of communication and day-to-day business activities. The implementation of these new Wireless devices also brings about new security threats to Information assets. This paper will determine the risks involved with new technologies and motivate the importance of understanding these risks before its implementation by emphasising the important role Corporate and IT Governance play.

KEY WORDS

Information Security, Corporate Governance, IT Governance, Wireless Technology, Risk Assessment, Compliance

THE PROLIFERATION OF WIRELESS DEVICES AND ITS EFFECTS ON CORPORATE GOVERNANCE

1 INTRODUCTION

Mobile computing along with Wireless Technology, is the next stage in the evolution of computing bringing about substantial benefits to both organisations and individuals. Wireless Local Area Networks (WLAN) are growing popular at a rapid rate, enabling users to access to vital information anywhere and anytime and proving to be both time and cost effective to organisations across many sectors. On the other hand, the implementation of Wireless Technology introduces new threats and risks to the information of the organisation and corporate assets that may have been previously overlooked. Organisations need to understand the importance of constantly securing their information, whether the information is stored locally, or accessed remotely.

Since its conception in 1980, many organisations are experimenting in implementing WLAN's using a variety of technologies; such as infrared and radio wave technology (Uskela, 1997). Corporate IT teams, with the introduction of wireless devices such as; Personal Digital Assistants (PDA'S), Laptops and Smartphones need to learn and adopt new security technologies and methodologies to target the unique requirements of the organisation. The IEEE 802.11 standard, which describes wideband wireless applications (Uskela, 1997), was sanctioned in 1997. Organisations are now implementing this standard to expand their physical reach. Wireless Technology enables businesses to create new partners compared to traditional wired technology which otherwise inhibits this expansion (Quay, 2002). The implementation of this technology allows users to work beyond the confines of the office by communicating over air waves. Additionally, wireless technology may cause a cost saving to the organisation by enabling network connections formerly that are too expensive to connect with physical connections (Quay, 2002).

Today almost every business aspect involves the use of IT. Organisations are investing large amounts of capital in implementing new technologies to create a broader spectrum of business associates. A greater capital gain and return on investment (ROI) is achieved with a broader reach. There are very few users and companies not utilising mobile devices whether it is a laptop or handheld device. This high usage of mobile devices requires great emphasis be placed on securing both the stored and communicated information. Security should be a priority as this information can contain valuable corporate data. It is imperative that users of mobile devices follow a mobile security policy, personal or corporate, to protect this data (Burling, 2005).

The objective of this paper is to identify the major risks of wireless devices and networks and its effects on corporate governance. The paper will secondly determine appropriate measures through which organisations can secure their information by understanding the importance of risk assessment before implementing new technologies. This will be accomplished by first identifying the threats to wireless technology and address ways in which organisations can safeguard their assets on a wireless network. The paper will then look at the Corporate Governance

and its effects and how it plays a role in securing stored and communicated information in a wireless environment.

2 TRENDS IN WIRELESS COMPUTING

Wireless Information Systems (WIS) are computing systems that enable users to work and collaborate from a remote location at anytime and any place (Katz, 1995).

The limitations for wireless include speed, quality of service and reliability. Businesses are implementing a wireless infrastructure to enable their employees to operate off-site leading to a high productive rate. A survey conducted by CIO Magazine in 2002 (Ware, 2002) reveals that since businesses moved from wired technology to a wireless technology, there was an increase of productivity. It revealed that there was a greater customer satisfaction and a greater ROI. The enablement of employees to operate on a more mobile basis aids with response time to customer and colleagues in real time (Burling, 2005).

Mobile devices are being incorporated into business systems, allowing users to access and communicate corporate data at any time or place. Users are no longer tied down to their office desks with the use of mobile devices. Employees can now work on the road or work whilst attending conferences by simply connecting to a wireless hotspot or access point. The use of wireless or mobile devices allows the user to be more flexible in terms of mobility which may lead to a higher productivity rate and reduced cost of ownership (Bluesocket, 2005).

Organizations today are deploying wireless technology at a rapid rate, often without considering all security aspects (Convery *et al.*, 2003). Wireless computing and wireless systems can be summarised as follows (V.Varadharajan, 2003):

- **User Mobility –** Users have access to files and network resources including the internet without having to be physically connected. This enables users to be mobile yet utilise the LAN with its high speeds in real time.
- **Rapid Installation –** Installation time is reduced because network connections can be made without making modifications to the existing physical infrastructure of the corporate LAN.
- **Flexibility –** System administrators can rapidly install a small WLAN for temporary needs such as a conference or meeting with minimal time wasted with implementing cables etc.
- **Scalability -** WLAN network topologies can easily be configured to meet specific application and installation needs and scaled from small peer-to-peer networks to very large enterprise networks that enable roaming over a broad area.

Wireless integration needs to be kept under constant review as wireless technology is fast becoming integrated into business processes. It is important for organisations, along with internal auditors and the board to develop adequate security strategies and understand the threats associated with wireless technology to ensure business survival.

3 TAXONOMY OF WIRELESS THREATS

All forms of network are vulnerable to attacks. The threats to IT security are fast becoming more costly to organizations, as more business processes are becoming computerized and becoming more mobile. Along with the vulnerabilities that face the traditional wired networks, wireless networks and devices introduce a new set of threats and risks. Wireless networks are more susceptible to attacks than traditional wired networks due to one fundamental flaw, a weak encryption standard called Wireless Equivalence Privacy, known as WEP. Attackers have easy access to mobile devices because they are not bound to the physical environment and can compromise the cornerstones of Information Security; Confidentiality, Integrity and Availability.

A thorough analysis of IT threats that can affect corporate data is therefore critical before the use of mobile devices can be accepted. WLAN has an open nature and can introduce a number of new and unknown threats compared to the more traditional wired LAN's. Information stored on mobile devices is therefore also open to attacks and new threats. Risk and threat can be analysed in two forms, passive and active attacks. Figure 1 below illustrates the levels of attacks which impact Wireless Networks.

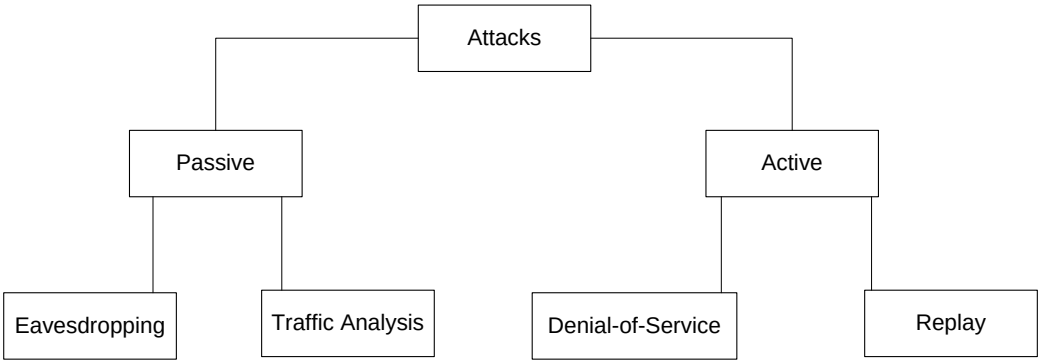

Figure 1: Types of Attacks in Wireless Networks

3.1 Passive Attacks

Passive attacks occur when unauthorised users gain entry into a system and do not alter the information or the original content. There are numerous forms of attacks which can occur on a passive basis, such as eavesdropping and traffic analysis.

3.1.1 Eavesdropping

Eavesdropping involves the process of users intercepting data over the air while being a distance away from the physical location (Quay, 2002). This form of attack may cost an organisation both financial loss and corporate identity, as it attacks the confidentiality of the information. This form of attack can be executed with minimal effort or equipment and without detection (Hiltunon 2003). The primary goal of the attacker is to understand:

- Who uses the network;
- What information is accessible;
- What the capabilities of the equipment on the network are;
- General usage of the equipment;

- What the coverage area of the equipment is.

The encryption standard, WEP, was introduced to secure information against this form of attack. This standard should be used as a minimum when securing corporate or personal data. A determined attacker can still log information being transmitted even with WEP turned on.

3.1.2 Traffic Analysis

Traffic analysis is a technique whereby the attacker can determine the load on the network by the number of packets being transmitted (Welch et al 2003). This form of attack is frequently used by attackers to gain access to the network before launching a malicious attack.

The attacker first determines the amount of activity across the network. If there is a substantial amount of network activity, it is a clear indication of a large event taking place with large amounts of data being transferred. The attacker may find the physical locations of Access Points (AP's) in the surrounding area. The final goal of traffic analysis is to determine the type of protocol being used in the transmission of data and can therefore be used in attacks against the identified protocol.

3.2 Active Attacks

Active attacks are attacks in which attackers gain access to the network and modify the stored data or disrupt network services and attack the network in real time.

3.2.1 Denial of Service Attacks (DoS)

Wireless networks are extremely vulnerable to DoS attacks. A DoS attack can force the speeds of the network to slow dramatically, or worse, disable the network all together therefore compromising the Availability of the information.

The protection of the network against this attack can be a costly exercise (Uskela, 1997). The only effective way to safeguard information is to isolate the network with heavy security. This solution is not practical unless the information stored on the network is of a highly sensitive nature (Geier, 2003). A viable solution to protect data against DoS attacks is to design, implement and maintain a strong Intrusion Detection Systems (IDS) to monitor the network activity and enforce a predefined security policy.

3.2.2 Replay Attacks

This form of attack is used to gain access to the network by convincing the host that a valid client needs to associate within the network. This attack is not executed in real time, which makes detection difficult. The original information obtained in a session is not altered or interfered in any way, but the attacker will have access to the network at a later stage. Replay attacks target the integrity of information by injecting incorrect data into the system.

Network administrators need to identify the threats associated with wireless networks and mobile devices to the organisations' information assets and resources. Securing wireless access requires securing the confidentiality; integrity and availability of information, only then can an organisation gather the benefits of a wireless network.

4 WIRELESS SECURITY

Many organisations are spending large amounts of money on implementing security for wired technologies by means of various firewall technologies and other security solutions. All wired and wireless networks cannot be kept secure against attacks especially when adding Wireless technology.

It is crucial that the organisations develop a Wireless Security policy as part of an overall security policy (Tyrrell, 2003). A security policy should be developed before a wireless network is initiated. Management can reduce costs that may incur later through developing a security policy at an early stage, followed by the implementation of stronger security mechanisms. A security policy will not eliminate wireless threats but will help create a proactive environment to combat these threats effectively (Farschi, 2003). When developing a security policy, the desired security should be reached by following the characteristics (Stanley, 2002):

- *Confidentiality* - The assurance that all information is kept secret and made only available to users who have access to the information;
- *Integrity* - The assurance that information is kept in its true form whether the data is in transit or at rest;
- *Authenticity* - The assurance that the information originates from the claimed entity.

Wireless Equivalency Protocol was introduced as a countermeasure to attacks to maintain the confidentiality and integrity of information. The initial intent for WEP was to prevent passive attacks such as eavesdropping from occurring. WEP ensures that only authorised users have access to the information.

There are two types of WEP keys, static and dynamic. Static keys are less secure than dynamic keys because there are fewer keys in use. Dynamic keys keep changing on a regular basis thus giving attackers less time to decode them. Static WEP should not be implemented as a standalone security mechanism and should be used in conjunction with other security controls such as Virtual Private Networks (VPN) or move to a dynamic WEP key system (Grimm, 2002). WEP has a weak data encryption mechanism and allows for keys to be decoded in a short period of time as there is no key management (Siska, 2004).

VPN technologies, such as IPSec, along with the use of an encryption algorithm, such as 3DES (Triple Data Encryption Standard), can protect the data by ensuring users are authenticated on the system and that their credentials are made available to all access points on the network. This ensures that the correct access policies are carried out by the authenticated user in the environment (Singhal, 2002).

Organisations that implement wireless technology should first investigate and assess the vendors to evaluate any plans for improving the WEP weakness (McCollum, 2002). Plans for improving the WEP standard include moving to a new standard increasing the data protection level and access control, called WiFi Protected Access (WPA) (Grimm, 2002). WPA provides a high level of assurance to its users in the protection of their data and that only authorised users may access the data (Grimm, 2002).

It is in the interest of senior management to implement best practices to secure the information stored on the network. A control mechanism such as WEP is a solution that is followed by conforming to best practices. It is implemented by means

of a framework which is discussed by senior management. Security controls can range from physical security, such as placement of the Access Points and network devices, to the human aspect such as loss or theft. It is important that senior management identify these possible security measures to maintain the securing of corporate data at all times. The aim of security is to inculcate a culture of transparency and accountability within the everyday workings of the entire workforce (SurfControl, 2004).

Indiscretion implementation of wireless devices and the utilisation of mobile devices can cause risks to a nature that business survival and continuity is threatened. Successful implementation of wireless network and the use of mobile devices is dependant on the understanding of the types of wireless threats and the impact the threats have on corporate information.

5 THE ROLE OF CORPORATE GOVERNANCE

It is essential for organisations to have an effective IT Governance strategy with the complexity and growth of IT along with its technologies. It is a strategy that dictates how the organisation is to be controlled and directed to align with overall organisational objectives.

The growth of technology demands an effective IT Governance strategy which dictates how an organisation should be controlled and directed to align and balance business goals. Sir Adrian Cadbury describes Corporate Governance as a framework to encourage the efficient use of resources and equally to require accountability for the stewardship of those resources (World Bank Group, 1999). Corporate Governance entails ensuring that corporate actions, agents and assets are directed at the constitutional objectives set out by the owners and shareholders (Sternberg, 2002).

Corporate Governance sets out a strategy for making strategic decisions in which distribution of rights and responsibilities is shared amongst participants such as: board of directors, shareholders and stakeholders. There is a distinct emphasis that security is a top-down approach and that management play a crucial role in securing corporate data. Executives and board of directors need to take a more active approach in securing information by educating users and increasing the level of awareness (Narendra, Kamat *et al.*). It is the responsibility of the board of directors and executive management to provide a secure environment for all users of the system to operate in a safe and controlled environment (ISACA, 2001). Governance is fast becoming more involved and essential in the business process, as more threats are being discovered and becoming more sophisticated.

There is an emphasis on the importance of good corporate governance practice. It is becoming crucial that organisations are compliant with current laws and regulations or face penalties such as legal action or financial loss (Computhink, 2004). These laws and regulation place a great responsibility and accountability to executives and board of directors. The company may face great financial loss or loss of corporate identity without the support of senior management and executives.

There have been many downfalls in the past due to poor corporate governance management, such as Enron Corp. and Tyco. At Enron, a gas pipeline giant, the board of directors failed to control conflicts of interest which were harmful to their shareholders' interest and failed to challenge questionable practices (Sternberg, 2002). Tyco, a manufacturer of undersea cables and fire sprinklers, had its downfall due to its

key figure, Dennis Kozlowski, accused of tax evasion (News Batch, 2004). The goal of good corporate governance practice is to ensure the entity's integrity. Many of the scandals have been a result of the lack of accountability and responsibility from the board of directors (Sternberg, 2002).

Information Technology presents itself with major risks as well as a competitive edge to the organisation over its competitors. Corporate Governance operates on a high level within the organisation and it is therefore important that the board direct and control the organisation by taking into consideration all expenses and threats. Every business process that is threatened needs to be taken into consideration to ensure business survival and therefore be placed high up on the business agenda. It is important for organisations to ensure that the identified risks are controlled in an appropriate manner by managing wireless networks and devices and following good Corporate Governance practices.

6 WIRELESS AND CORPORATE GOVERNANCE

Information security is often considered a set of technical issues, but should rather be embraced as a Corporate Governance issue that involves responsibility, risk management, reporting controls, testing and training and executive accountability (Swindle and Conner, 2004).

Organizations should utilize a risk management process to assess the risks involved, before establishing wireless networks and using mobile devices to take steps to reduce the risks to an acceptable level and to maintain that acceptable level of risk (Radack, 2003). The use of a risk management processes can assist managers in protecting systems and information in a cost-effective manner by balancing the operational and economic costs of the protective measures against the gains in mission capability achieved through the application of new technology (Radack, 2003).

The success of deploying a successful network and implementing new technology is dependant on the co-operation between management and IT specialists and this is where IT Governance plays an important role (Oak, 2002). IT governance is an inclusive term that includes:

- Information systems, technology and communication;
- Business legal and other issues;
- All concerned stakeholders.

The COBIT (Control Objectives for Information and related Technology) Framework describes IT governance as providing the structure that links IT processes, IT resources and information to enterprise strategies and objectives (Oak, 2002). It integrates optimal ways of planning and organizing, acquiring and implementing, delivering and supporting, and monitoring IT performance. Essentially, governance addresses proper management of organisations (Spafford, 2003).

It is important for senior management to work along side with IT Specialists to moderate and mitigate risks performing a risk assessment and analysis of the network (Kennedy, 2004) before the implementation of new technologies. The completion of a risk analysis and assessment gives an understanding of what threats can occur and the impact of these risks. It is important that the organisation constantly monitor and

control any activity and the information, stored or communicated. The constant change and evolution of wireless requires administrators to proactively measure and analyse network resources and signal to ensure security is kept at a maximum (Geier, 2004). It is critical that organisations understand the impact of risks and threats with the constant change and evolution of technologies

In section 4, it was pointed out that wireless security is an essential process to ensure the business survival and continuity by limiting risks placed on the corporate information. In section 5, it was highlighted that it is important for senior management and the board direct and control risks and ensure the business survival by controlling risks. Therefore, the indiscretion proliferation of wireless devices should be considered a board issue. Highly sensitive information is communicated on wireless networks and is used on mobile devices. It is up to the board to ensure that adequate measure are in place to ensure the safeguarding of information.

7 CONCLUSION

New technologies such as wireless network and wireless devices are posing a great security threat to organisations due to the inherent risks of vetting employees (Nel, 2005) and the more traditional risks. Senior management needs to understand the risk to safeguard information and to keep information confidential (Confidentiality), in its true and original form (Integrity) and always be made available (Availability). It is important for the organisation to implement policies and procedures to address, assess and monitor risks and for the board of directors to assure that the controls in place are functioning appropriately (Stout, 2005). Securing any network, wired or wireless requires a top down analysis of requirements, a risk assessment and the development of a well defined security policy, followed by the correct implementation of the security measures (NextComm Inc, 2002). It is clear that corporate governance and IT governance play a crucial role in establishing a secure wireless infrastructure to ensure business alignment and following best business practices by taking into consideration that security should be considered a top down approach.

8 REFERENCE:

Bluesocket, Inc (2005). Selection and Deployment Issues for Wireless LAN's: Early Due Diligence can Result in a Successful and Effective Network. Retrieved 05 May 2005, from http://www.itresearch.forbes.com/detail/RES/1115743995_49.html

Burling, D. (2005). Defining a Security Policy for Windows Mobile Pocket PC. Retrieved 03 March 2005, from http://www.geekzone.co.nz/content.asp?contentid=3909

Convery, S., Miller, D., & Sundaralingam, S. (2003). Cisco Safe: Wireless LAN Security in Depth. Retrieved 28 March 2005, from http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.pdf

Computhink. (2004). Compliance Becomes a Top Concern. Retrieved 17 March 2005, from http://knowledgestorm.co.nz/shared/write/collateral/WTP/3881_93336_41969_Computhink_Compliancy.pdf

Credant. (2005). SOX, GLB, SB 1386 and Mobile Devices - Are you at Risk for Non-compliance? Retrieved 15 March 2005, from http://research.bizreport.com/detail/RES/1107364149_56.html

Farschi, J. (2003). Wireless Network Policy Development. Retrieved 17 March 2005, from http://www.securityfocus.com/infocus/1732

Geier, J. (2004). Implementing WLAN Analysis. Retrieved 03 April 2005, from http://www.wi-fiplanet.com/tutorials/article.php/3388501

Grimm, C. B. (2002). WiFi's Protected Access Wireless: The Background. Retrieved 01 April 2005, from http://www.newswireless.net/index.cfm/article/528

ISACA. (2001). Information Security Governance - Guidance for Board of Directors and Executive Management. Retrieved 04 April, 2005, from http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Information_Security_Governance_Guidance_for_Boards_of_Directors_and_Executive_Management/infosecurity.pdf

Katz, R. H. (1995). Adaptation and Mobility in Wireless Information Systems. Retrieved 02 March 2005, from http://zoo.cs.yale.edu/classes/cs434/readings/papers/katz94.pdf

Kennedy, S. (2004). Best Practices for Wireless Network Security. Retrieved 04 April 2005, from http://www.computerworld.com/mobiletopics/mobile/story/0,10801,86951,00.html

McCollum, T. (2002). Wireless Security. Retrieved 01 April 2005, from http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=501

Narendra Kamat, Lee, H., Li, B., & Menchaca, D. Evolution of Wireless LAN Security Standards.

Nel, S. (2005) Wireless Technology a new threat to digital security? Retrieved 12 April 2005, from http://www.securitysa.com/news.asp?pklNewsID=16746&pklIssueID=467&pklCategoryID=11

News Batch. (2004). Corporate Responsibility. Retrieved 14 April 2005, from http://www.newsbatch.com/corp.htm

NextComm Inc. (2002). Security in Wireless Networks. Retrieved 01 April 2005, from http://www.nextcomm.com/security_white_paper.pdf

Oak, P. (2002). Deploying Wireless Technology--A Case for IT Governance. Retrieved 03 April 2005, from http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=17033&TEMPLATE=/ContentManagement/ContentDisplay.cfm

Quay, D. C. H. (2002, 21 February 2002). Formulating a Wireless LAN Security Policy: Relevant Issues, Considerations and Implications. Retrieved 20 February 2005, from http://www.giac.org/practicals/David_Quay_GSEC.doc

Radack, S. (2003). Security for Wireless Network and Devices. Retrieved 14 April 2005, from http://www.itl.nist.gov/lab/bulletns/bltnmar03.htm

Singhal, S. (2002, 25 November 2002). Plugging Holes in your Wireless LAN. Retrieved 01 April 2005, from http://wirelessreview.com/wifi/wireless_plugging_holes_wireless/

Siska, A. (2004). Deploying Secure Wireless LAN's. Retrieved 29 March 2005, from http://cisco.parsek.tv/si/ibm_lj/03.pdf

Spafford, G. (2003). The Benefits of Standard IT Governance Frameworks. Retrieved 17 March 2005, from http://itmanagement.earthweb.com/netsys/article.php/2195051

Stanley, R. A. (2002). Wireless LAN Risks and Vulnerabilities. Retrieved 01 April 2005, from http://cnscenter.future.co.kr/resource/hot-topic/wlan/wirelesswhitepaper.pdf

Sternberg, E. (2002). The Corporate Governance Implications of Enron. Retrieved 14 April 2005, from http://www.iea.org.uk/files/upl-article43pdf?.pdf

Stout, H. (2005). The Board's Role in Compliance. Retrieved 14 April 2005, from http://www.fredlaw.com/articles/corporate/stout0503.pdf

SurfControl. (2004). Changing Attitudes: A UK White Paper on Corporate Governance. Retrieved 01 April 2005, from http://www.surfcontrol.com/uploadedfiles/general/white_papers/CorporateGovernance-UK.pdf

Swindle, O, Conner, Conner B. (2004). The Link between Information Security and Corporate Governance. Retrieved 14 April 2005, from http://www.computerworld.com/securitytopics/security/story/0,10801,92915p2,00.html

Tyrrell, K. (2003). An Overview of Wireless Security Issues. Retrieved 02 April 2005, from http://www.giac.org/certified_professionals/practicals/gsec/2471.php

Uskela, S. (1997). Security in Wireless Local Area Networks. Retrieved 04 March 2005, from http://www.tml.hut.fi/Opinnot/Tik-110.501/1997/wireless_lan.html

V.Varadharajan. (2003). Wireless Security with an Emphasis on WEP. Retrieved 28 March 2005, from http://engr.smu.edu/~jseraj/2003_termpapers/Venkataraman%20Term%20Paper%20latest.doc

Ware, L. C. (2002). Wireless Update - Slow and Steady Progress. Retrieved 24 March 2005, from http://www2.cio.com/research/surveyreport.cfm?id=36